(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年2 月19 日 (19.02.2004)

PCT

(10) 国際公開番号
WO 2004/015916 A1

(51) 国際特許分類[7]: H04L 9/06, G09C 1/00

(21) 国際出願番号: PCT/JP2003/010186

(22) 国際出願日: 2003 年8 月8 日 (08.08.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-231284 2002 年8 月8 日 (08.08.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 福岡 俊彦 (FUKUOKA,Toshihiko) [JP/JP]; 〒575-0061 大阪府 四条畷市 清滝中町１５−２４ Osaka (JP). 和田 妙美 (WADA,Taemi) [JP/JP]; 〒572-0013 大阪府 寝屋川市 三井が丘４−４−８２−４０６ Osaka (JP).

(74) 代理人: 前田 弘, 外(MAEDA,Hiroshi et al.); 〒550-0004 大阪府 大阪市 西区靭本町１丁目４番８号 本町中島ビル Osaka (JP).

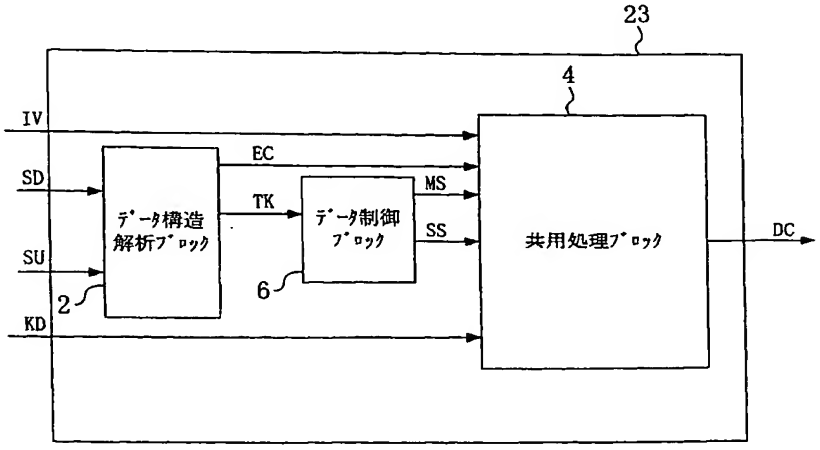
(81) 指定国 (国内): CN, JP, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

(54) Title: ENCRYPTING/DECRYPTING DEVICE AND METHOD, ENCRYPTING DEVICE AND METHOD, DECRYPTING DEVICE AND METHOD, AND TRANSMITTING/RECEIVING DEVICE

(54) 発明の名称: 暗号化復号化装置及び方法、暗号化装置及び方法、復号化装置及び方法、並びに送受信装置



2... DATA STRUCTURE ANALYZING BLOCK
6... DATA CONTROL BLOCK
4... SHARED PROCESSING BLOCK

(57) Abstract: An encrypting/decrypting device comprises a data structure analyzing block that receives encrypted data or data to be encrypted and that outputs, as processing-block input data, control data and the encrypted data or data to be encrypted; a data control block that obtains and outputs a mode selection signal in accordance with the control data; and a shared processing block that encrypts or decrypts the processing-block input data and outputs the resultant. The shared processing block is adapted to perform an ECB processing using input key data so that it can perform encryption and decryption in any one of CBC and CFB modes. The shared processing block, therefore, performs an encryption or decryption in a mode indicated by the mode selection signal.

[続葉有]

WO 2004/015916 A1

(57) 要約:　暗号化復号化装置として、暗号化データ又は暗号化すべきデータを受け取り、制御用データ、及び、暗号化データ又は暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、制御用データに従ってモード選択信号を求めて出力するデータ制御ブロックと、処理ブロック入力データに対して暗号化又は復号化を行い、得られた結果を出力する共用処理ブロックとを備える。共用処理ブロックは、入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、モード選択信号に示されたモードで暗号化又は復号化を行う。

明　細　書

暗号化復号化装置及び方法、暗号化装置及び方法、復号化装置及び方法、並びに送受信装置

技術分野

本発明は、暗号化及び暗号の復号化技術に関する。

背景技術

デジタル双方向通信の代表的な例である双方向ＣＡＴＶ（cable television）システムでは、暗号化機能を実現するために、ＴＶ端末には暗号化機能が実装される。この暗号化機能としては、ＤＥＳ（data encryption standard）暗号に代表される秘密鍵暗号方式と、ＲＳＡ（Rivest-Shamir-Adleman）暗号に代表される公開鍵暗号方式とを組み合わせた方式が用いられる。

秘密鍵暗号方式とは、暗号化と復号化とに用いる鍵が共通であり、暗号化に用いられた鍵を用いて暗号化アルゴリズムを逆の順に実行することによって復号化を行い、暗号化を施す前の原文を得る方式である。この方式は、単純な排他的論理和の繰り返しアルゴリズムで実現されるもので、高速な処理を可能とする反面、送信側と受信側とで共通の鍵を保有する必要があり、鍵の配送・保持が困難であるという特徴を有する。

公開鍵暗号方式とは、落とし戸関数と呼ばれる、関数の演算は容易に実行でき、逆関数の演算を行うのは非常に困難であるような関数を利用するものであり、暗号化と復号化とに使用する鍵が異なるものである。したがって、鍵の配送・保持は容易に行える反面、秘密鍵暗号方式に比べて計算が複雑であり、秘密鍵暗号方式と比較して暗号化・復号化により多くの処理時間を要する。ただし、公開鍵暗号方式を使用して認証及び鍵配送を行い、秘密鍵暗号方式を使用してデータの暗

号化を行うことによって、それぞれの利点を生かすことが可能となる。

さて、米国の標準方式であるＤＥＳ暗号方式では、ＥＣＢ（electronic code book）モードと呼ばれる、入力データサイズが６４ビット、出力データサイズが６４ビットの演算を基本処理として行う。この暗号方式の暗号化アルゴリズムに対して、あらかじめ文字又は単語が出現する頻度の分布を統計処理しておけば、入手した暗号化文の文字列パターンの頻度分布とのマッチングをとることにより、暗号化前の平文が推定されてしまう可能性がある。

そこで、暗号化された６４ビットの暗号ブロックと次に入力される６４ビットの入力データとの排他的論理和を演算して暗号文を作成する方法が考え出された。この方法を行って暗号化するモードをＣＢＣ（cipher block chaining）モードと呼んでいる。また、パケット通信のように通信を行う際のデータ単位があらかじめ決められている場合があるが、６４ビットを１ブロックとするブロック暗号化方式では、１ブロックのビット数（６４ビット）で割り切れないデータ単位が入力された場合には、１ブロックに満たない端数データができる。

データに端数部分がある場合には、１つ前のブロックの暗号解読演算結果と端数データの排他的論理和演算を実行し暗号化する。このような端数処理を行うモードの１つとして、ＣＦＢ（cipher feedback）モードがあり、ＣＦＢモードによって、データが６４ビットに満たない場合でも暗号文を得ることができる。

また、暗号化及び暗号解読（復号化）のいずれの演算においても、通常は５６ビットのデータを鍵として用いるが、特定の条件下では、４０ビットのデータを鍵として用いるモードも存在する。この場合、他のモードの場合と同様に、演算処理自体は６４ビット単位で行うが、鍵の有効データが４０ビットとなる。

このように、秘密鍵暗号方式演算においては複数のモード、すなわち、ＥＣＢモード、ＣＢＣモード及びＣＦＢモードのうちの１つと、５６ビット鍵モード又は４０ビット鍵モードのいずれかとの組み合わせに対応したモードが存在する。そして、デジタル双方向通信のセキュリティ機能を実現するために、すべてのモードに対応した暗号化装置又は復号化装置が一般的に用いられる。

関連する技術が、例えば米国特許第５，８３５，５９９号明細書に開示されている。

－解決課題－

従来のＤＥＳ暗号方式に基づく暗号化装置又は復号化装置は、複数のモードのそれぞれのための回路を備え、システムの要求に応じて複数のモードのいずれかを適宜選択し、そのモードのための回路を用いて暗号化演算又は暗号解読演算を行う構成となっている。

ところが、近年、暗号化又は暗号解読を必要とするシステムでは、単一の鍵のみを使用する場合は少なく、複数の鍵を使用して、それぞれの鍵に対応した演算を行う場合も増加してきている。

これを実現する装置は、各モードごとの暗号化又は暗号解読機能を備えた上、複数の鍵に対する演算を行う機能も必須となり、回路規模は莫大なものとなる。一般的に、複数の鍵に対する演算は並列実行する必要があるため、処理が必要となる鍵の数が増大すると、装置としても、鍵の数に応じた数の処理回路を有する必要がある。

しかし、ＤＥＳの各モードは、ＥＣＢ処理と呼ばれる、ＤＥＳの基本処理を変形した処理が行われるものである。また、各モードを同時に並列実行する場合はほとんどない。このため、暗号化装置及び復号化装置において、複数のモードで処理回路を共用化して回路規模を削減することは可能である。

発明の開示

本発明は、複数の暗号モードで処理回路を共用化することによって、回路規模を削減した暗号化復号化装置、暗号化装置、復号化装置、及び送受信装置を提供することを目的とする。

本発明の暗号化復号化装置は、暗号化データ又は暗号化すべきデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロッ

ク入力データとして出力するデータ構造解析ブロックと、前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを備え、前記共用処理ブロックは、入力された鍵データを用いたＥＣＢ（electronic code book）処理を行うことによって、ＣＢＣ（cipher block chaining）モード及びＣＦＢ（cipher feedback）モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである。

これによると、複数の暗号モードでの暗号化及び復号化の処理を共用処理ブロックによって実現することができるので、暗号モード毎に処理回路を設ける必要がない。したがって、暗号化復号化装置の回路面積を削減して、そのコストを抑えることができる。

また、本発明の暗号化装置は、暗号化すべきデータを受け取り、そのデータ構造の解析を行って、制御用データを求めて出力するとともに、前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、前記処理ブロック入力データに対して暗号化を行い、得られた暗号化結果を出力する共用処理ブロックとを備え、前記共用処理ブロックは、入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化を行うものである。

また、本発明の復号化装置は、暗号化データを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記

暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、前記処理ブロック入力データに対して復号化を行い、得られた復号化結果を出力する共用処理ブロックとを備え、前記共用処理ブロックは、入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで復号化を行うものである。

また、本発明の送受信装置は、受信した信号をデータに変換して出力するダウンストリームＰＨＹ部と、前記データからダウンストリームデータ及び鍵データを分離して出力するダウンストリームデータ処理部と、前記鍵データを用いて前記ダウンストリームデータを復号化して出力する第１の暗号化復号化装置と、前記復号化されたダウンストリームデータを格納する記憶部と、前記記憶部から読み出されたアップストリームデータを暗号化して出力する第２の暗号化復号化装置と、前記暗号化されたアップストリームデータに、暗号化に用いられた鍵データを付加して出力するアップストリームデータ処理部と、前記アップストリームデータ処理部が出力するデータを信号に変換して送信するアップストリームＰＨＹ部とを備え、前記第１及び第２の暗号化復号化装置は、いずれも、暗号化データを含む前記ダウンストリームデータ又は暗号化すべきデータを含む前記アップストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブ

ロックとを有するものであり、前記共用処理ブロックは、入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである。

－発明の効果－

以上のように、本発明によると、同一のハードウェアによって多くの暗号モードにおいて暗号化／復号化を行うことができるので、回路面積を削減してコストを抑えることができる。多くの機能を低コストで提供することができるので、暗号化復号化装置等のコストパフォーマンスを高めることができる。

図面の簡単な説明

図１は、本発明の実施形態に係る暗号化復号化装置の構成を示すブロック図である。

図２は、図１の共用処理ブロックの構成の例を示すブロック図である。

図３は、図１の共用処理ブロックが行う処理の流れを示す説明図である。

図４は、図１の共用処理ブロックの第１～第４のセレクタが選択するデータの組み合わせを示す説明図である。

図５は、本発明の実施形態に係る暗号化復号化装置の他の構成の例を示すブロック図である。

図６は、図１の暗号化復号化装置を用いた送受信装置のブロック図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について、図面を参照しながら説明する。

図１は、本発明の実施形態に係る暗号化復号化装置の構成を示すブロック図である。図１の暗号化復号化装置２３は、データ構造解析ブロック２と、共用処理ブロック４と、データ制御ブロック６とを備えている。以下では例として、図１の暗号化復号化装置２３は、センター装置及び複数の端末装置により構成される

双方向通信網において、端末装置の１つに含まれるものであるとして説明するが、センター装置に含まれていてもよい。センター装置は、暗号化されたデータを含むダウンストリームデータＳＤを端末装置に送信する。ダウンストリームデータＳＤには、映像データ及び伝送制御データが含まれている。一方、端末装置は、暗号化すべきデータを含むアップストリームデータを受け取り、暗号化してセンター装置に対して送信する。

データ構造解析ブロック２は、ダウンストリームデータＳＤを受け取り、その構文解析を行う。ダウンストリームデータＳＤは、例えば、映像データにおけるＭＰＥＧ（moving picture experts group）構造と、ＭＰＥＧ構造に埋め込まれているネットワーク処理用のサブレイヤであるＭＡＣ（media access control）構造を有している。

まず、データ構造解析ブロック２は、ＭＰＥＧ構造データ中のヘッダ部分を解析し、ＭＡＣ構造データを抜き出すための情報を抽出した後に、ＭＡＣ構造データを抜き出す。次に、ＭＡＣ構造データ中のヘッダ部分を解析し、通常のヘッダのみでなく、拡張ヘッダと呼ばれる拡張されたフィールドが存在する場合は、この拡張ヘッダを解析する。拡張ヘッダは、データ構成の拡張を可能にするものであって、暗号化の有無、その他の暗号化又は復号化のための処理に必要となる情報を有している。

拡張ヘッダが存在しない場合、データ構造解析ブロック２は、ダウンストリームデータＳＤが暗号化されていないと判断する。この場合、データ構造解析ブロック２は、ＴＥＫ（traffic encryption key）制御用データＴＫを例えば値“０”に固定し、データ制御ブロック６に出力する。

拡張ヘッダが存在する場合、データ構造解析ブロック２は、暗号化に関する情報を格納するフィールドを解析する。暗号化されていないことを確認した場合には、拡張ヘッダが存在しない場合と同様の処理を行う。暗号化されていることを確認した場合には、暗号化に関する情報であるＳＩＤ（service ID）及びキーシーケンスナンバー（key sequence number）を拡張ヘッダから抽出し、ＴＥＫ制

御用データＴＫとしてデータ制御ブロック６に出力する。

また、データ構造解析ブロック２は、暗号化すべきデータをアップストリームデータＳＵとして受け取り、そのデータ構造の解析を行う。データ構造解析ブロック２は、アップストリームデータＳＵに含まれるデータからＳＩＤ及びキーシーケンスナンバーを抽出し、ＴＥＫ制御用データＴＫとしてデータ制御ブロック６に出力する。

データ構造解析ブロック２は、ダウンストリームデータＳＤに含まれるＭＰＥＧ構造を有する暗号化データ、又はアップストリームデータＳＵに含まれる暗号化すべきデータを、処理ブロック入力データＥＣとして共用処理ブロック４に出力する。

データ構造解析ブロック２は、受信したダウンストリームデータＳＤ又はアップストリームデータＳＵのパケットのビット数をカウントし、ストリームのパケットのビット数が６４ビット以下、６４ビットの倍数、又は６４ビットの倍数と６４ビット以下の端数との和のいずれであるか、及びパケットのうち処理ブロック入力データＥＣとして出力したビット数（パケットカウント）を求める。データ構造解析ブロック２は、求められた結果、並びに、ダウンストリームデータＳＤを受け取った場合には復号化すべきであることを、及びアップストリームデータＳＵを受け取った場合には暗号化すべきであることをもＴＥＫ制御用データＴＫとしてデータ制御ブロック６に出力する。

次に、データ制御ブロック６は、データ構造解析ブロック２から受信したＴＥＫ制御用データＴＫを用いて処理を行う。まず、ＳＩＤ及びキーシーケンスナンバーをチェックして、これらのデータがあらかじめ決められている有効な数値であるかどうかを判断する。無効な数値であると判断した場合は、何も処理を行わない。有効な数値であると判断した場合は、データ制御ブロック６は、５６ビット鍵モードであるか否かをチェックする。暗号化及び復号化には、５６ビットの鍵が標準として用いられるが、これ以外の長さの鍵も用いられる。以下では例として、５６ビット又は４０ビットの鍵が用いられるものとする。５６ビット鍵モ

ードであるか否かは、ＳＩＤ及びキーシーケンスナンバーに一意に対応する。データ制御ブロック６は、５６ビット鍵モードであるか否かを示す情報をモード選択信号ＭＳとして出力する。

データ制御ブロック６は、ＴＥＫ制御用データＴＫに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号ＳＳを共用処理ブロック４に出力する。また、データ制御ブロック６は、ＴＥＫ制御用データＴＫを参照して、処理ブロック入力データＥＣのパケットのビット数が６４ビット以下の場合はＣＦＢモードを示す信号を、６４ビットの倍数である場合はＣＢＣモードを示す信号を、モード選択信号ＭＳとして共用処理ブロック４に出力する。

パケットのビット数が６４ビットの倍数と６４ビット以下の端数との和である場合は、データ制御ブロック６は、パケットカウントに応じて、モード選択信号ＭＳを次のように切り替える。すなわち、データ構造解析ブロック２が６４ビットの倍数に相当する処理ブロック入力データＥＣを出力しているときは、ＣＢＣモードを示す信号を、６４ビット以下の端数に相当する処理ブロック入力データＥＣを出力しているときは、ＣＦＢモードを示す信号を、データ制御ブロック６がモード選択信号ＭＳとして出力する。また、データ制御ブロック６は、それぞれのモードの処理を開始する初期状態、又はその後の定常状態のいずれであるかも、モード選択信号ＭＳとして出力する。

また、データ構造解析ブロック２は、受信したダウンストリームデータＳＤ又はアップストリームデータＳＵに応じて、ＥＣＢモードで処理すべきか否かをＴＥＫ制御用データＴＫによってデータ制御ブロック６に通知する。ＥＣＢモードで処理すべき場合には、データ制御ブロック６は、ＥＣＢモードを示す信号をモード選択信号ＭＳとして出力する。

このように、データ制御ブロック６は、ＳＩＤ、キーシーケンスナンバー、及びパケットカウント等に応じてモード選択信号ＭＳを切り替えて、共用処理ブロック４に出力する。

共用処理ブロック４は、複数の暗号モードにおける処理に共通に用いられる。

すなわち、共用処理ブロック４は、外部から入力された初期ベクタデータＩＶ、及び鍵データＫＤを用いたＥＣＢ処理を行うことによって、ＥＣＢモード、ＣＢＣモード及びＣＦＢモードのいずれの暗号モードにおいても、処理ブロック入力データＥＣに対して暗号化及び復号化を行うことができるように構成されている。共用処理ブロック４は、モード選択信号ＭＳに示されたモードで、暗号化／復号化切り替え信号ＳＳに従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を処理済データＤＣとして出力する。

図２は、図１の共用処理ブロック４の構成の例を示すブロック図である。図２の共用処理ブロック４は、第１のセレクタ４１と、第２のセレクタ４２と、第３のセレクタ４３と、第４のセレクタ４４と、ビットマスク器４６と、ＥＣＢ処理器４７と、遅延器４８と、排他的論理和演算器４９とを備えている。

第１のセレクタ４１は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号ＭＳに従って、処理ブロック入力データＥＣ、及びＥＣＢ処理器４７が出力する暗号処理データＰＤのうちのいずれかを選択して排他的論理和演算器４９に出力する。

遅延器４８は、処理ブロック入力データＥＣ、及び暗号処理データＰＤを入力とし、それぞれを、ＥＣＢ処理器４７が６４ビットのデータに対してＥＣＢ処理を行うのに要する時間だけ遅延させて、第２のセレクタ４２に出力する。

第２のセレクタ４２は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号ＭＳに従って、処理ブロック入力データＥＣ、初期ベクタデータＩＶ、並びに、遅延器４８が出力する遅延した処理ブロック入力データＥＣＤ及び遅延した暗号処理データＰＤＤのうちのいずれかを選択して排他的論理和演算器４９に出力する。

排他的論理和演算器４９は、第１のセレクタ４１の出力と第２のセレクタ４２の出力との排他的論理和を対応するビット毎に求めて第４のセレクタ４４に出力する。

第３のセレクタ４３は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号

ＭＳに従って、処理ブロック入力データＥＣ、排他的論理和演算器４９が出力する排他的論理和データＥＲ、遅延した処理ブロック入力データＥＣＤ、及び遅延した暗号処理データＰＤＤのうちのいずれかを選択してＥＣＢ処理器４７に出力する。

ビットマスク器４６は、鍵データＫＤを、モード選択信号ＭＳに従って必要に応じてその一部をマスクして、モードに適合した鍵データとしてＥＣＢ処理器４７に出力する。

第４のセレクタ４４は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号ＭＳに従って、暗号処理データＰＤ及び排他的論理和演算器４９が出力する排他的論理和データＥＲのうちのいずれかを選択して、暗号化結果又は復号化結果として出力する。

ＥＣＢ処理器４７は、暗号化／復号化切り替え信号ＳＳ及びモード選択信号ＭＳに従って、ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを、第３のセレクタ４３の出力に対して行う。ＥＣＢ処理器４７は、ビットマスク器４６が出力するモードに適合した鍵データを用いてＥＣＢ処理を行い、得られた結果を暗号処理データＰＤとして第１のセレクタ４１、第４のセレクタ４４、及び遅延器４８に出力する。

図３は、図１の共用処理ブロック４が行う処理の流れを示す説明図である。図３において、上段は暗号化処理の流れを示し、下段は復号化処理の流れを示している。処理Ｅ１，Ｅ２，Ｅ３，Ｅ９，Ｄ１，Ｄ２，Ｄ３，Ｄ９はそれぞれＥＣＢ処理を表している。共用処理ブロック４は、暗号化処理及び復号化処理のいずれの場合にも、ＣＢＣモードによる処理を行う必要があるときは、ＣＢＣモードによる処理を連続して行い、その後、必要に応じてＣＦＢモードによる処理を行う。

図３では、処理Ｅ９，Ｄ９を含む最も右の列の処理はＣＦＢモードの処理を示している。処理Ｅ１，Ｅ２，Ｅ３，Ｄ１，Ｄ２，Ｄ３を含むその他の３つの列の処理はＣＢＣモードの処理を示している。また、「ＩＶ」は初期ベクタデータ、「Ｄ」は暗号化されていないデータ、「Ｉ」は、図３上段の暗号化処理の場合は

ＥＣＢ処理前、下段の復号化処理の場合はＥＣＢ処理後のデータを示す。また、「Ｃ」は暗号化データ、「Ｅｎｃｒｙｐｔ」はＥＣＢ処理器４７におけるＥＣＢ処理が暗号化処理であること、「Ｄｅｃｒｙｐｔ」はＥＣＢ処理器４７におけるＥＣＢ処理が復号化処理であることを示す。実際のＥＣＢ処理には鍵データを用いるが、図３においては、鍵データのデータフローは省略している。図３の処理の流れは、５６ビット鍵モードであるか否かにかかわらず同様である。

図４は、図１の共用処理ブロック４の第１～第４のセレクタ４１～４４が選択するデータの組み合わせを示す説明図である。共用処理ブロック４の復号化処理時の動作について、図２、図３の下段、及び図４を参照して説明する。この場合、共用処理ブロック４には、暗号化／復号化切り替え信号ＳＳとして、復号化を示す信号が入力される。５６ビット鍵モードであるか否か、ＣＢＣモード及びＣＦＢモードのうちのいずれであるか、初期状態及び定常状態のうちのいずれであるかによって場合を分けて説明する。ＥＣＢ処理器４７におけるＥＣＢ処理は、ＣＢＣモードの場合は復号化処理、ＣＦＢモードの場合は暗号化処理である。

１）５６ビット鍵モードであり、かつ、ＣＢＣモードの初期状態である場合（図４のＤＥＣ－ＣＢＣ　Ｉｎｉｔの場合）

この場合は、図３の下段の処理Ｄ１及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック４は、暗号化データＣを入力とし、ＥＣＢ処理として「Ｄｅｃｒｙｐｔ」処理を行って、データＩを求める。共用処理ブロック４は、求められたデータＩと入力された初期ベクタデータＩＶとの排他的論理和を求めて、暗号化されていないデータＤとして出力する。

この場合の処理を、図２を参照して説明する。共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＢＣモードの初期状態であることを示す信号が入力される。

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、初期ベクタデータＩＶを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと初期ベクタデータＩＶ

との排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

第３のセレクタ４３は、処理ブロック入力データＥＣを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された処理ブロック入力データＥＣに対してＥＣＢ処理として復号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして復号化結果を出力する。

２）５６ビット鍵モードであり、かつ、ＣＢＣモードの定常状態である場合（図４のＤＥＣ－ＣＢＣ　Ｎｏｒｍａｌの場合）

この場合は、図３の下段の処理Ｄ２又はＤ３及びこれらのそれぞれに続く排他的論理和を求める処理が行われる。共用処理ブロック４は、暗号化データＣを入力とし、「Ｄｅｃｒｙｐｔ」処理を行って、データＩを求める。共用処理ブロック４は、求められたデータＩとその前のＥＣＢ処理で用いた暗号化データＣとの排他的論理和を求めて、暗号化されていないデータＤとして出力する。

この場合の処理を、図２を参照して説明する。共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＢＣモードの定常状態であることを示す信号が入力される。

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、遅延器４８が出力する遅延された処理ブロック入力データＥＣＤを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと遅延された処理ブロック入力データＥＣＤとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

第３のセレクタ４３は、処理ブロック入力データＥＣを選択してＥＣＢ処理器

４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された処理ブロック入力データＥＣに対してＥＣＢ処理として復号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして復号化結果を出力する。

３）５６ビット鍵モードではなく、かつ、ＣＢＣモードの初期状態である場合

４）５６ビット鍵モードではなく、かつ、ＣＢＣモードの定常状態である場合

これらの場合は、それぞれ１），２）の場合と次の点を除いて同じである。すなわち、共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードではないことを示す信号が入力される。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードではないことを示す信号が入力されているので、入力された５６ビットの鍵データＫＤのうち、必要がないビット（例えば上位１６ビット）をマスクして、４０ビット鍵データとしてＥＣＢ処理器４７に出力する。ＥＣＢ処理器４７は、ビットマスク器４６から出力された４０ビット鍵データを用いてＥＣＢ処理を行う。

５）５６ビット鍵モードであり、かつ、ＣＦＢモードの初期状態である場合（図４のＤＥＣ－ＣＦＢ　Ｉｎｉｔの場合）

ＣＦＢモードの処理のみを行うときには、ＣＦＢモードの初期状態における処理が行われる。この場合は、図３の下段の処理Ｄ９及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック４は、暗号化データＣを入力とし、「Ｅｎｃｒｙｐｔ」処理を行って、データＩを求める。共用処理ブロック４は、求められたデータＩと入力された初期ベクタデータＩＶデータとの排他的論理和を求めて、暗号化されていないデータＤとして出力する。

この場合の処理を、図２を参照して説明する。共用処理ブロック４には、モー

ド選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＦＢモードの初期状態であることを示す信号が入力される。

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、初期ベクタデータＩＶを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと初期ベクタデータＩＶとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

第３のセレクタ４３は、処理ブロック入力データＥＣを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された処理ブロック入力データＥＣに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして復号化結果を出力する。

６）５６ビット鍵モードであり、かつ、ＣＦＢモードの定常状態である場合（図４のＤＥＣ－ＣＦＢ　Ｎｏｒｍａｌの場合）

ＣＢＣモードの処理に続いてＣＦＢモードの処理を行うときには、ＣＦＢモードの定常状態における処理が行われる。この場合は、図３の下段の処理Ｄ９及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック４は、その前のＥＣＢ処理で用いた暗号化データＣを入力とし、「Ｅｎｃｒｙｐｔ」処理を行って、データＩを求める。共用処理ブロック４は、求められたデータＩと次の暗号化データＣとの排他的論理和を求めて、暗号化されていないデータＤとして出力する。

この場合の処理を、図２を参照して説明する。共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＦＢモードの定

常状態であることを示す信号が入力される。

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、処理ブロック入力データＥＣを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと処理ブロック入力データＥＣとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

第３のセレクタ４３は、遅延器４８が出力する遅延された処理ブロック入力データＥＣＤを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された遅延された処理ブロック入力データＥＣＤに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして復号化結果を出力する。

７）５６ビット鍵モードではなく、かつ、ＣＦＢモードの初期状態である場合

８）５６ビット鍵モードではなく、かつ、ＣＦＢモードの定常状態である場合

これらの場合は、それぞれ５），６）の場合と次の点を除いて同じである。すなわち、共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードではないことを示す信号が入力される。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードではないことを示す信号が入力されているので、入力された５６ビットの鍵データＫＤのうち、必要がないビット（例えば上位１６ビット）をマスクして、４０ビット鍵データとしてＥＣＢ処理器４７に出力する。ＥＣＢ処理器４７は、ビットマスク器４６から出力された４０ビット鍵データを用いてＥＣＢ処理を行う。

共用処理ブロック４の暗号化処理時の動作について、図２、図３の上段、及び

図４を参照して説明する。この場合、共用処理ブロック４には、暗号化／復号化切り替え信号ＳＳとして、暗号化を示す信号が入力される。５６ビット鍵モードであるか否か、ＣＢＣモード及びＣＦＢモードのうちのいずれであるか、初期状態及び定常状態のうちのいずれであるかによって場合を分けて説明する。ＥＣＢ処理器４７におけるＥＣＢ処理は、ＣＢＣモードの場合及びＣＦＢモードの場合ともに暗号化処理である。

９）５６ビット鍵モードであり、かつ、ＣＢＣモードの初期状態である場合（図４のＥＮＣ－ＣＢＣ　Ｉｎｉｔの場合）

この場合は、図３の上段の処理Ｅ１及びその前の排他的論理和を求める処理が行われる。共用処理ブロック４は、入力された初期ベクタデータＩＶと暗号化されていないデータＤとの排他的論理和を求めて、データＩとして出力する。共用処理ブロック４は、得られたデータＩにＥＣＢ処理として「Ｅｎｃｒｙｐｔ」処理を行って、暗号化データＣを求めて出力する。

この場合の処理を、図２を参照して説明する。共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＢＣモードの初期状態であることを示す信号が入力される。

第１のセレクタ４１は、処理ブロック入力データＥＣを選択して出力する。第２のセレクタ４２は、初期ベクタデータＩＶを選択して出力する。排他的論理和演算器４９は、処理ブロック入力データＥＣと初期ベクタデータＩＶとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

第３のセレクタ４３は、排他的論理和データＥＲを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された排他的論理和データＥＲに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４

のセレクタは、暗号処理データＰＤを選択して、処理済データＤＣとして暗号化結果を出力する。

１０）５６ビット鍵モードであり、かつ、ＣＢＣモードの定常状態である場合（図４のＥＮＣ－ＣＢＣ　Ｎｏｒｍａｌの場合）

この場合は、図３の上段の処理Ｅ２又はＥ３及びこれらのそれぞれの前の排他的論理和を求める処理が行われる。共用処理ブロック４は、暗号化されていないデータＤとその前のＥＣＢ処理で得られた暗号化データＣとの排他的論理和を求めて、データＩとして出力する。共用処理ブロック４は、得られたデータＩにＥＣＢ処理として「Ｅｎｃｒｙｐｔ」処理を行って、暗号化データＣを求めて出力する。

この場合の処理を、図２を参照して説明する。共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＢＣモードの定常状態であることを示す信号が入力される。

第１のセレクタ４１は、処理ブロック入力データＥＣを選択して出力する。第２のセレクタ４２は、遅延器４８が出力する遅延された暗号処理データＰＤＤを選択して出力する。排他的論理和演算器４９は、処理ブロック入力データＥＣと遅延された暗号処理データＰＤＤとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

第３のセレクタ４３は、排他的論理和データＥＲを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された排他的論理和データＥＲに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、暗号処理データＰＤを選択して、処理済データＤＣとして暗号化結果を出力する。

１１）５６ビット鍵モードではなく、かつ、ＣＢＣモードの初期状態である場合

１２）５６ビット鍵モードではなく、かつ、ＣＢＣモードの定常状態である場合

これらの場合は、それぞれ９），１０）の場合と次の点を除いて同じである。すなわち、共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードではないことを示す信号が入力される。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードではないことを示す信号が入力されているので、入力された５６ビットの鍵データＫＤのうち、必要がないビット（例えば上位１６ビット）をマスクして、４０ビット鍵データとしてＥＣＢ処理器４７に出力する。ＥＣＢ処理器４７は、ビットマスク器４６から出力された４０ビット鍵データを用いてＥＣＢ処理を行う。

１３）５６ビット鍵モードであり、かつ、ＣＦＢモードの初期状態である場合（図４のＥＮＣ－ＣＦＢ　Ｉｎｉｔの場合）

ＣＦＢモードの処理のみを行うときには、ＣＦＢモードの初期状態における処理が行われる。この場合は、図３の上段の処理Ｅ９及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック４は、暗号化されていないデータＤを入力とし、「Ｅｎｃｒｙｐｔ」処理を行う。共用処理ブロック４は、この処理で求められたデータと入力された初期ベクタデータＩＶデータとの排他的論理和を求めて、暗号化データＣとして出力する。

この場合の処理を、図２を参照して説明する。共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＦＢモードの初期状態であることを示す信号が入力される。

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、初期ベクタデータＩＶを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと初期ベクタデータＩＶとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲ

を出力する。

第３のセレクタ４３は、処理ブロック入力データＥＣを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された処理ブロック入力データＥＣに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして暗号化結果を出力する。

１４）５６ビット鍵モードであり、かつ、ＣＦＢモードの定常状態である場合（図４のＥＮＣ－ＣＦＢ　Ｎｏｒｍａｌの場合）

ＣＢＣモードの処理に続いてＣＦＢモードの処理を行うときには、ＣＦＢモードの定常状態における処理が行われる。この場合は、図３の上段の処理Ｅ９及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック４は、その前のＥＣＢ処理で得られた暗号化データＣを入力とし、「Ｅｎｃｒｙｐｔ」処理を行う。共用処理ブロック４は、この処理で求められたデータと暗号化されていないデータＤとの排他的論理和を求めて、暗号化データＣとして出力する。

この場合の処理を、図２を参照して説明する。共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードであること、及びＣＦＢモードの定常状態であることを示す信号が入力される。

第１のセレクタ４１は、ＥＣＢ処理器４７が出力する暗号処理データＰＤを選択して出力する。第２のセレクタ４２は、処理ブロック入力データＥＣを選択して出力する。排他的論理和演算器４９は、暗号処理データＰＤと処理ブロック入力データＥＣとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データＥＲを出力する。

第３のセレクタ４３は、遅延器４８が出力する遅延された暗号処理データＰＤ

Ｄを選択してＥＣＢ処理器４７に出力する。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードであることを示す信号が入力されているので、入力された５６ビットの鍵データＫＤをマスクせずにそのままＥＣＢ処理器４７に出力する。

ＥＣＢ処理器４７は、ビットマスク器４６から出力された５６ビット鍵データを用いて、第３のセレクタから出力された遅延された暗号処理データＰＤＤに対してＥＣＢ処理として暗号化処理を行い、得られた暗号処理データＰＤを出力する。第４のセレクタは、排他的論理和演算器４９が出力する排他的論理和データＥＲを選択して、処理済データＤＣとして暗号化結果を出力する。

１５）５６ビット鍵モードではなく、かつ、ＣＦＢモードの初期状態である場合

１６）５６ビット鍵モードではなく、かつ、ＣＦＢモードの定常状態である場合

これらの場合は、それぞれ１３），１４）の場合と次の点を除いて同じである。すなわち、共用処理ブロック４には、モード選択信号ＭＳとして、５６ビット鍵モードではないことを示す信号が入力される。ビットマスク器４６は、モード選択信号ＭＳとして５６ビット鍵モードではないことを示す信号が入力されているので、入力された５６ビットの鍵データＫＤのうち、必要がないビット（例えば上位１６ビット）をマスクして、４０ビット鍵データとしてＥＣＢ処理器４７に出力する。ＥＣＢ処理器４７は、ビットマスク器４６から出力された４０ビット鍵データを用いてＥＣＢ処理を行う。

なお、モード選択信号ＭＳがＥＣＢモードを示す場合には、第３のセレクタ４３は処理ブロック入力データＥＣを選択して出力し、かつ、第４のセレクタ４４は暗号処理データＰＤを選択して出力する。ＥＣＢ処理器４７は、暗号化／復号化切り替え信号ＳＳが、暗号化を示す場合は暗号化処理を行い、復号化を示す場合は復号化処理を行う。すなわち、図１の暗号化復号化装置は、ＣＢＣモード及びＣＦＢモードに加えてＥＣＢモードにおける暗号化及び復号化を行うことがで

きる。

また、５６ビット鍵データ又は４０ビット鍵データに代えて、他の長さの鍵データを用いるようにすることも容易にできる。

また、図１の暗号化復号化装置を暗号化装置として用いるようにしてもよい。この場合は、入力されたダウンストリームデータを暗号化して出力するのみでよく、以上の説明における復号化に対応した構成及び動作は不要である。また、暗号化／復号化切り替え信号ＳＳは不要であり、第１～第４のセレクタ及びＥＣＢ処理器は、モード選択信号ＭＳに従って動作すればよい。

より具体的には、遅延器は、暗号処理データＰＤを入力とし、これを遅延させて出力する。第２のセレクタは、処理ブロック入力データＥＣ、初期ベクタデータＩＶ、及び遅延器が出力する遅延した暗号処理データＰＤＤのうちのいずれかを選択して出力する。第３のセレクタは、処理ブロック入力データＥＣ、排他的論理和演算器が出力する排他的論理和データＥＲ、及び遅延した暗号処理データＰＤＤのうちのいずれかを選択して出力する。第４のセレクタは、暗号処理データＰＤ及び排他的論理和データＥＲのうちのいずれかを選択して、暗号化結果として出力する。

また、図１の暗号化復号化装置を復号化装置として用いるようにしてもよい。この場合は、入力されたアップストリームデータを復号化して出力するのみでよく、以上の説明における暗号化に対応した構成及び動作は不要である。このため、暗号処理データＰＤを常に出力する第１のセレクタ、及び排他的論理和演算器が出力する排他的論理和データＥＲを常に出力する第４のセレクタは不要である。また、暗号化／復号化切り替え信号ＳＳは不要であり、第２及び第３のセレクタ及びＥＣＢ処理器は、モード選択信号ＭＳに従って動作すればよい。

より具体的には、遅延器は、処理ブロック入力データＥＣを入力とし、これを遅延させて出力する。第２のセレクタは、処理ブロック入力データＥＣ、初期ベクタデータＩＶ、及び遅延器が出力する遅延した処理ブロック入力データＥＣＤのうちのいずれかを選択して出力する。第３のセレクタは、処理ブロック入力デ

ータＥＣ、及び遅延した処理ブロック入力データＥＣＤのうちのいずれかを選択して出力する。排他的論理和演算器は、暗号処理データＰＤと第２のセレクタの出力との排他的論理和を求めて、復号化結果として出力する。

また、本発明は、ＣＰＵやＤＳＰ（digital signal processor）等のプロセッサを用いたソフトウェアによる処理を行うことによって実現することも可能である。

以上のように、本発明に係る暗号化復号化装置によると、モード選択信号を変化させれば、ＥＣＢモード、ＣＢＣモード及びＣＦＢモードのうちのいずれかと、５６ビット鍵モード又は４０ビット鍵モードのいずれかとを組み合わせたいずれのモードにおいても、同一のハードウェアによって暗号化データに対する復号化を行い、暗号解読データを得ることができる。

また、暗号化／復号化切り替え信号を変化させれば、いずれのモードにおいても、データの暗号化及び復号化のいずれをも、同一のハードウェアによって行うことができる。したがって、暗号化復号化装置の回路規模の削減を図ることができる。

図５は、本発明の実施形態に係る暗号化復号化装置の他の構成の例を示すブロック図である。図５の暗号化復号化装置は、データ構造解析ブロック２０２と、共用処理ブロック４と、データ制御ブロック２０６と、第１及び第２の入力セレクタ２０７，２０８と、出力セレクタ２０９とを備えている。図５の暗号化復号化装置は、トリプルＤＥＳ（triple DES）方式による暗号化及び復号化を行う装置である。共用処理ブロック４は、図１を参照して説明したものと同様のものである。

データ構造解析ブロック２０２は、図１のデータ構造解析ブロック２と同様の動作を行う他、入力されたストリームデータのヘッダから、このストリームデータをトリプルＤＥＳ方式で処理すべきか否かを判断し、その結果をもＴＥＫ制御用データＴＫとしてデータ制御ブロック２０６に出力する。

データ制御ブロック２０６は、図１のデータ制御ブロック６と同様の動作を行

う他、ＴＥＫ制御用データＴＫに基づいて、トリプルＤＥＳ方式で暗号化又は復号化すべきである場合には、トリプルＤＥＳモードを示す信号をもモード選択信号ＭＳとして共用処理ブロック４、入力セレクタ２０７及び２０８に出力する。また、データ制御ブロック２０６は、出力制御信号ＯＳを出力セレクタ２０９に出力する。

入力セレクタ２０７は、モード選択信号ＭＳに従って、ダウンストリームデータＳＤ又は共用処理ブロック４が出力する処理済データＤＣを選択し、データ構造解析ブロック２０２に出力する。入力セレクタ２０８は、モード選択信号ＭＳに従って、アップストリームデータＳＵ又は処理済データＤＣを選択し、データ構造解析ブロック２０２に出力する。出力セレクタ２０９は、出力制御信号ＯＳに従って、処理済データＤＣ又は値“０”を選択し、図５の暗号化復号化装置の処理済データＴＤとして出力する。

図５の暗号化復号化装置がトリプルＤＥＳモードで動作する際の動作について説明する。データ制御ブロック２０６は、通常は、ダウンストリームデータＳＤ及びアップストリームデータＳＵをそれぞれ選択するように、入力セレクタ２０７，２０８にモード選択信号ＭＳを出力し、処理済データＤＣを選択するように、出力セレクタ２０９に出力制御信号ＯＳを出力する。

共用処理ブロック４は、入力されたダウンストリームデータＳＤ又はアップストリームデータＳＵに対して１回目の処理を行い、処理済データＤＣを入力セレクタ２０７，２０８、出力セレクタ２０９に出力する。

モード選択信号ＭＳがトリプルＤＥＳモードを示す場合には、入力セレクタ２０７，２０８は、処理済データＤＣを選択する。このとき、出力セレクタ２０９は、出力制御信号ＯＳに従って、“０”を選択する。すると、共用処理ブロック４によって１回目の処理が行われた処理済データＤＣが、再びデータ構造解析ブロック２０２に入力され、共用処理ブロック４によって２回目の処理が行われる。

入力セレクタ２０７，２０８、出力セレクタ２０９は、その後も同様の選択を行うので、共用処理ブロック４によって２回目の処理が行われた処理済データＤ

Ｃが、再びデータ構造解析ブロック２０２に入力され、共用処理ブロック４によって３回目の処理が行われる。

３回目の処理が終了すると、出力セレクタ２０９は、処理済データＤＣを選択するので、トリプルＤＥＳ方式で暗号化又は復号化の処理が行われた結果が処理済データＴＤとして出力される。このとき、入力セレクタ２０７，２０８は、ダウンストリームデータＳＤ及びアップストリームデータＳＵをそれぞれ選択する。共用処理ブロック４における３回の処理のそれぞれとしては、暗号化及び復号化のうちのいずれをも行うようにすることができる。特に、暗号化、復号化、暗号化の順に処理を行うと、トリプルＤＥＳ方式による暗号化を行うことができ、復号化、暗号化、復号化の順に処理を行うと、トリプルＤＥＳ方式による復号化を行うことができる。

このように、図５の暗号化復号化装置によると、共用処理ブロック４において暗号化又は復号化処理を３回行うので、トリプルＤＥＳ方式による暗号化又は復号化を行うことができる。

なお、共用処理ブロック４における処理を、３回よりも多くの回数行うようにしてもよい。

図６は、図１の暗号化復号化装置を用いた送受信装置のブロック図である。図６の送受信装置１００は、ＰＨＹ部１０と、ＭＡＣ部２０と、画像処理部３２と、インタフェース部３４と、チューナ５２とを備えている。

ＰＨＹ部１０は、ダウンストリームＰＨＹ部１１と、アップストリームＰＨＹ部１２とを備えている。ＭＡＣ部２０は、ダウンストリームデータ処理部２１と、アップストリームデータ処理部２２と、暗号化復号化装置２３，２４と、ＣＰＵ２６と、記憶部２８とを備えている。暗号化復号化装置２３，２４は、いずれも、図１の暗号化復号化装置と同様のものである。なお、暗号化復号化装置２３，２４として、図５の暗号化復号化装置を用いてもよい。

受信時には、チューナ５２は、送信に使われるチャネルから１つを選択し、センター装置８０から送信された信号を低い周波数の信号に変換して、ダウンスト

リームＰＨＹ部１１に出力する。ダウンストリームＰＨＹ部１１は、受け取った信号をベースバンド信号に変換し、更にデータへの変換、及び誤り訂正を行って、ダウンストリームデータ処理部２１に出力する。

ダウンストリームデータ処理部２１は、受け取ったデータから、そのヘッダの情報に応じてダウンストリームデータＳＤ、鍵データＫＤ、初期ベクタデータＩＶ等を分離して、暗号化復号化装置２３に出力する。暗号化復号化装置２３は、図１を参照して説明したように、暗号に対する復号化を行い、得られた処理済データＤＣをバス２９に出力する。ＣＰＵ２６は、バス２９を経由して、処理済データＤＣを記憶部２８に格納させる。

ＣＰＵ２６は、記憶部２８からデータを読み出し、画像処理部３２に与える。画像処理部３２は、受け取ったデータに対して画像として表示させるために必要な処理を行い、得られたデータをインタフェース部３４を介して表示器（図示せず）に出力し、表示させる。

送信時には、ＣＰＵ２６は、記憶部２８からデータを読み出し、バス２９を経由して、暗号化復号化装置２４にアップストリームデータＳＵとして与える。暗号化復号化装置２４は、図１を参照して説明したように、受け取ったデータに対する暗号化を行い、得られた処理済データＤＣをアップストリームデータ処理部２２に出力する。アップストリームデータ処理部２２は、受け取ったデータにヘッダを付加する等の処理を行い、アップストリームＰＨＹ部１２に出力する。アップストリームＰＨＹ部１２は、受け取ったデータを電気信号に変換し、更にこれを送信に用いられる周波数に変換して、センター装置８０に送信する。

このように、図６の送受信装置によると、複数のモードにおける暗号化、又は複数のモードにおける復号化を、それぞれ同一のハードウェアによって行うので、回路規模の削減を図ることができる。

産業上の利用可能性

本発明に係る暗号化復号化装置及び方法は、多くの機能を低コストで提供する

ことができ、例えば、送受信装置や、データの記録再生装置等における暗号化及び暗号の復号化に有用である。

請 求 の 範 囲

１．　暗号化データ又は暗号化すべきデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

入力された鍵データを用いたＥＣＢ（electronic code book）処理を行うことによって、ＣＢＣ（cipher block chaining）モード及びＣＦＢ（cipher feedback）モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである

暗号化復号化装置。

２．　請求項１に記載の暗号化復号化装置において、

前記データ構造解析ブロックは、

前記暗号化データにおけるヘッダの解析を行い、前記ヘッダの情報に基づいて前記暗号化データからＭＡＣ（media access control）構造を抜き出し、前記ＭＡＣ構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該暗号化データが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記制御用データとして出力するとともに、前記ＭＡＣ構造デ

ータから前記拡張ヘッダを除去して前記処理ブロック入力データとして出力するものである

ことを特徴とする暗号化復号化装置。

３．　請求項１に記載の暗号化復号化装置において、

前記データ制御ブロックは、

前記制御用データに従って、前記処理ブロック入力データをＣＢＣモード、及びＣＦＢモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示す信号を前記モード選択信号として出力するものである

ことを特徴とする暗号化復号化装置。

４．　請求項１に記載の暗号化復号化装置において、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、

前記処理ブロック入力データ、及び前記暗号処理データを入力とし、それぞれを遅延させて出力する遅延器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延器が出力する遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、

前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果として出力する第４のセレクタとを備え、

前記ＥＣＢ処理器は、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする暗号化復号化装置。

５．　請求項４に記載の暗号化復号化装置において、

前記ビットマスク器は、

前記モード選択信号が５６ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとして出力するものである

ことを特徴とする暗号化復号化装置。

６．　請求項４に記載の暗号化復号化装置において、

前記第１のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前

記処理ブロック入力データを選択して出力し、その他の場合には、前記暗号処理データを選択して出力するものである
ことを特徴とする暗号化復号化装置。

７．　請求項４に記載の暗号化復号化装置において、
前記第２のセレクタは、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択して出力し、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力し、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択して出力し、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力するものである
ことを特徴とする暗号化復号化装置。

８．　請求項４に記載の暗号化復号化装置において、
前記第３のセレクタは、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であ

って、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

９．　請求項４に記載の暗号化復号化装置において、

前記第４のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合には、前記排他的論理和演算器の出力を選択して出力するものである

ことを特徴とする暗号化復号化装置。

１０．　請求項４に記載の暗号化復号化装置において、

前記ＥＣＢ処理器は、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合には、暗号化処理を行い、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、復号化処理を行い、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、暗号化処理を行うものである

ことを特徴とする暗号化復号化装置。

１１．　請求項１に記載の暗号化復号化装置において、

暗号化データ又は前記共用処理ブロックの出力を選択し、前記データ構造解析ブロックに出力する第１の入力セレクタと、

暗号化すべきデータ又は前記共用処理ブロックの出力を選択し、前記データ構造解析ブロックに出力する第２の入力セレクタと、

所定の値又は前記共用処理ブロックの出力を選択し、出力する出力セレクタとを更に備え、

前記暗号化データ又は前記暗号化すべきデータに対して前記共用処理ブロックにおける処理が所定の回数行われると、前記出力セレクタが前記共用処理ブロックの出力を選択するように構成されている

ことを特徴とする暗号化復号化装置。

１２．　請求項１１に記載の暗号化復号化装置において、

前記所定の回数は、３回である

ことを特徴とする暗号化復号化装置。

１３．　暗号化すべきデータを受け取り、そのデータ構造の解析を行って、制御用データを求めて出力するとともに、前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

前記処理ブロック入力データに対して暗号化を行い、得られた暗号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化を行うものである

暗号化装置。

１４．　請求項１３に記載の暗号化装置において、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、

前記暗号処理データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、

前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理

和演算器の出力、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果として出力する第４のセレクタとを備え、

前記ＥＣＢ処理器は、

前記ＥＣＢ処理として暗号化処理を前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする暗号化装置。

１５．　暗号化データを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

前記処理ブロック入力データに対して復号化を行い、得られた復号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで復号化を行うものである

復号化装置。

１６．　請求項１５に記載の復号化装置において、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記処理ブロック入力データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した処理ブロック入力データのうちのいずれかを選択して出力する第２のセレクタと、

前記暗号処理データと前記第２のセレクタの出力との排他的論理和を求めて、前記復号化結果として出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器とを備え、

前記ＥＣＢ処理器は、

前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする復号化装置。

１７．　受信した信号をデータに変換して出力するダウンストリームＰＨＹ部と、

前記データからダウンストリームデータ及び鍵データを分離して出力するダウンストリームデータ処理部と、

前記鍵データを用いて前記ダウンストリームデータを復号化して出力する第１の暗号化復号化装置と、

前記復号化されたダウンストリームデータを格納する記憶部と、

前記記憶部から読み出されたアップストリームデータを暗号化して出力する第２の暗号化復号化装置と、

前記暗号化されたアップストリームデータに、暗号化に用いられた鍵データを付加して出力するアップストリームデータ処理部と、

前記アップストリームデータ処理部が出力するデータを信号に変換して送信するアップストリームＰＨＹ部とを備え、

前記第１及び第２の暗号化復号化装置は、いずれも、

暗号化データを含む前記ダウンストリームデータ又は暗号化すべきデータを含む前記アップストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを有するものであり、

前記共用処理ブロックは、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである

送受信装置。

１８．　暗号化データ又は暗号化すべきデータのデータ構造の解析を行って、

暗号化に関する情報を制御用データとして求めるとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして求めるデータ構造解析ステップと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替えデータと、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データとを求めるデータ制御ステップと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替えデータに従って暗号化又は復号化を行って、暗号化結果又は復号化結果を求める共用処理ステップとを備え、

前記共用処理ステップは、

鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うものであり、前記モード選択データに示されたモードで暗号化又は復号化を行うものである

暗号化復号化方法。

１９．　暗号化すべきデータのデータ構造の解析を行って、制御用データを求めるとともに、前記暗号化すべきデータを処理ブロック入力データとして求めるデータ構造解析ステップと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めるデータ制御ステップと、

前記処理ブロック入力データに対して暗号化を行って、暗号化結果を求める共用処理ステップとを備え、

前記共用処理ステップは、

鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるものであり、前記モード選択データに示されたモードで暗号化を行うものである

暗号化方法。

２０．　暗号化データのデータ構造の解析を行って、暗号化に関する情報を制御用データとして求めるとともに、前記暗号化データを処理ブロック入力データとして求めるデータ構造解析ステップと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めて出力するデータ制御ステップと、

前記処理ブロック入力データに対して復号化を行って、復号化結果を求める共用処理ステップとを備え、

前記共用処理ステップは、

鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるものであり、前記モード選択データに示されたモードで復号化を行うものである

復号化方法。

FIG. 1

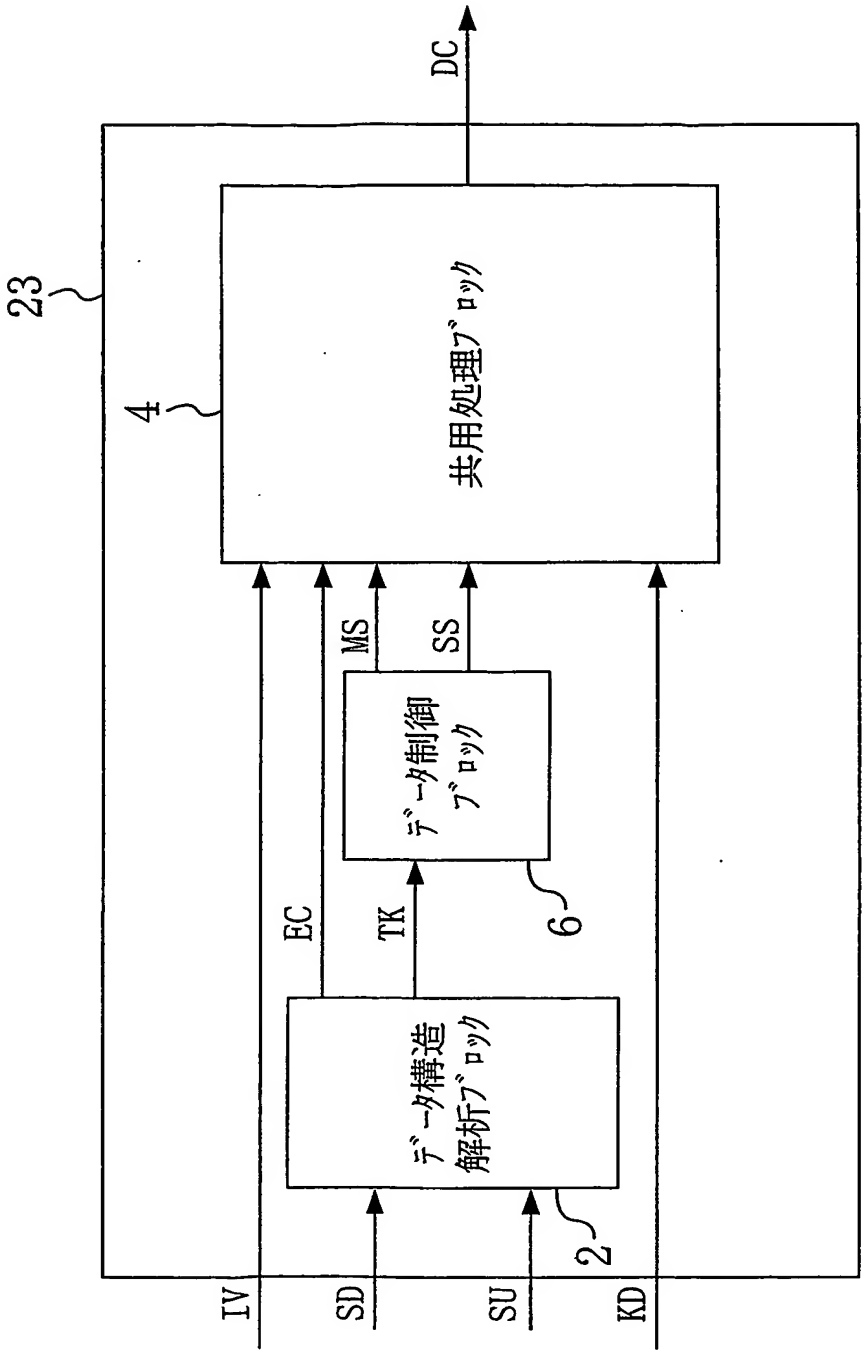

DC
23
4
共用処理ブロック
MS
SS
データ制御ブロック
6
EC
TK
データ構造解析ブロック
2
IV
SD
SU
KD

FIG. 2

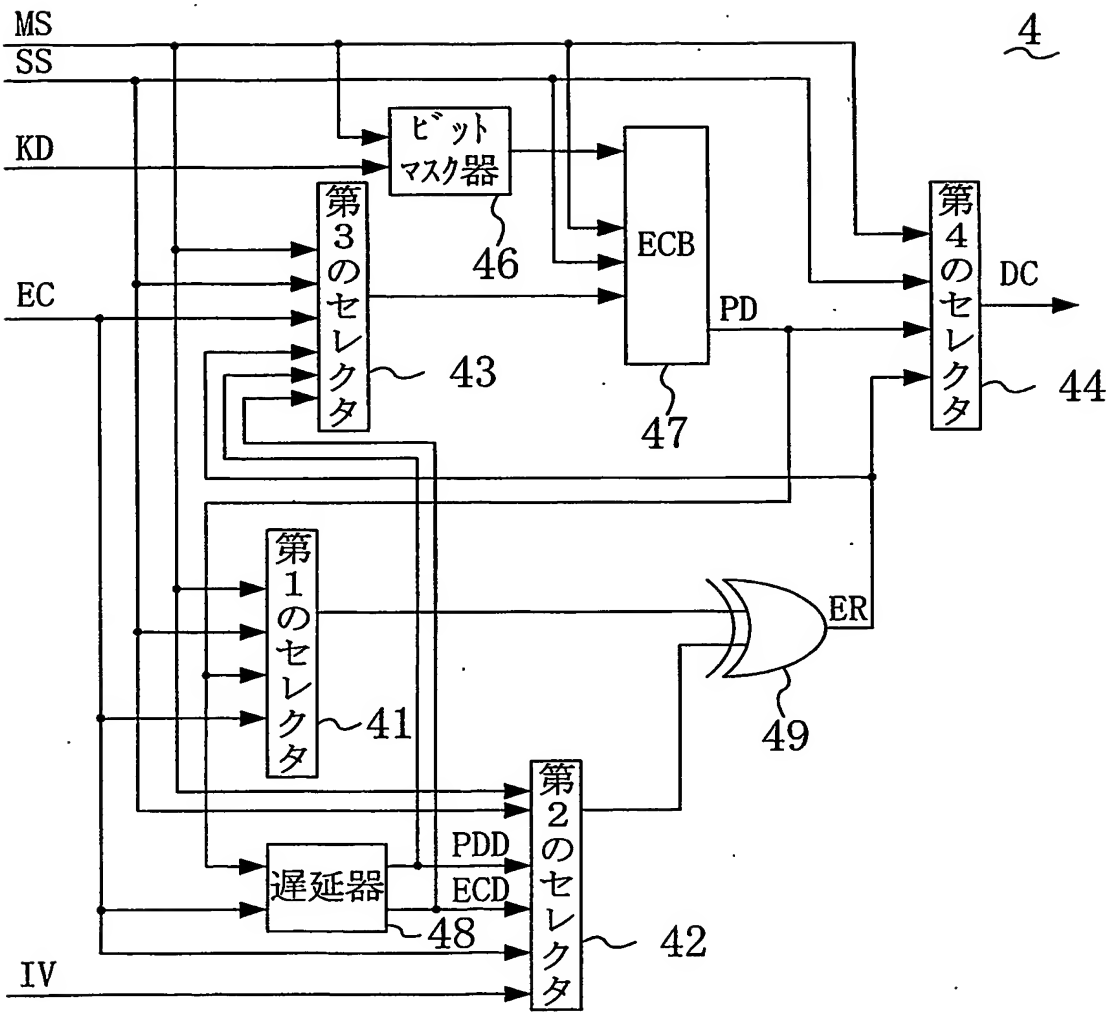

MS
SS
KD
EC
IV
ビット
マスク器
46
第3のセレクタ
43
ECB
47
PD
第4のセレクタ
44
DC
4
第1のセレクタ
41
ER
49
第2のセレクタ
42
PDD
ECD
遅延器
48

FIG. 3

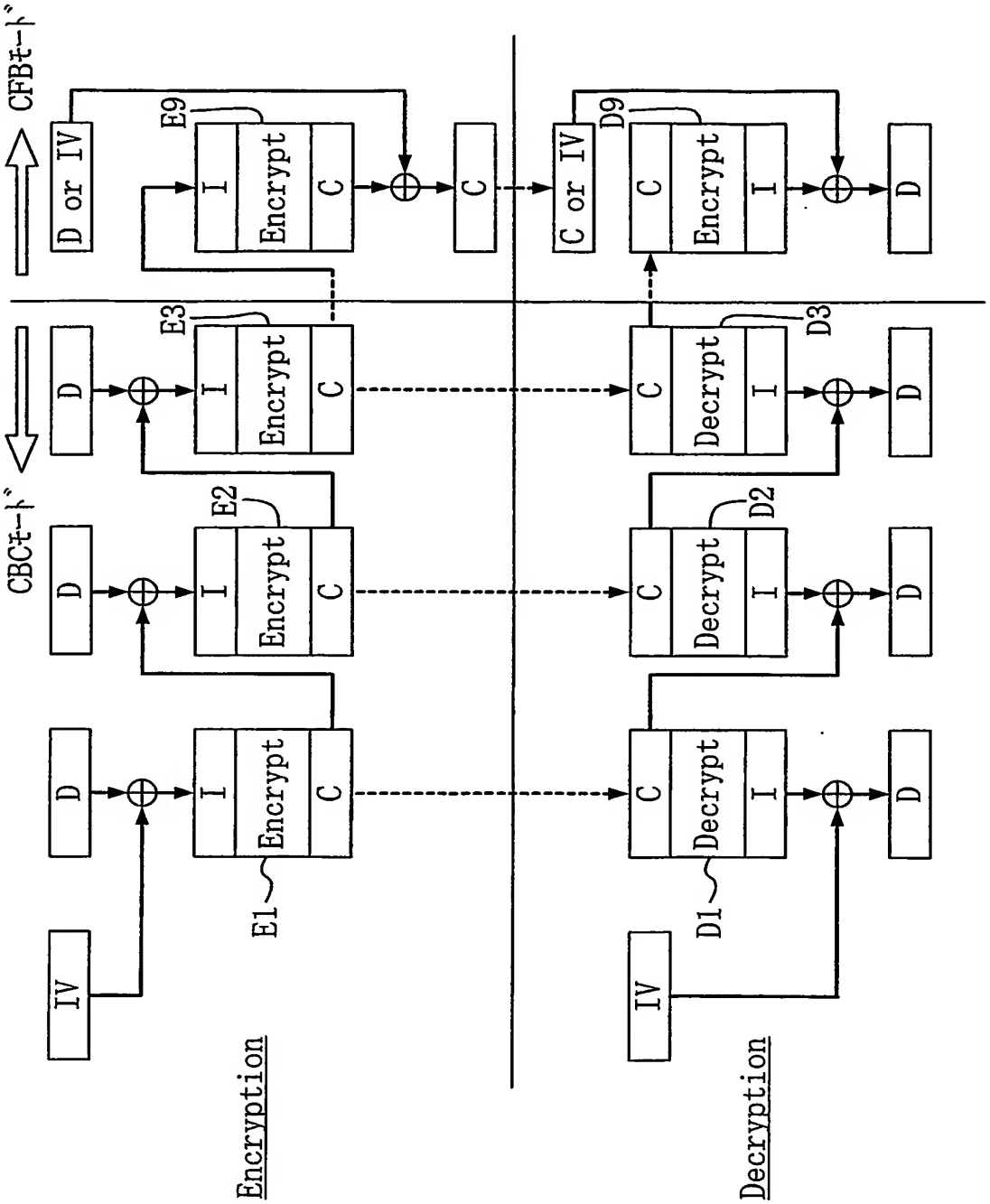

CFBモード
D or IV
E9
I
Encrypt
C
C
C or IV
D9
C
Encrypt
I
D
CBCモード
D
E3
I
Encrypt
C
C
Decrypt
I
D3
D
D
E2
I
Encrypt
C
C
Decrypt
I
D2
D
D
I
Encrypt
C
C
Decrypt
I
D
D
IV
E1
D1
IV
Encryption
Decryption

FIG. 4

	DEC-CBC Init	DEC-CBC Normal	DEC-CFB Init	DEC-CFB Normal	ENC-CBC Init	ENC-CBC Normal	ENC-CFB Init	ENC-CFB Normal
第1のセレクタ	PD	PD	PD	PD	EC	EC	PD	PD
第2のセレクタ	IV	ECD	IV	EC	IV	PDD	IV	EC
第3のセレクタ	EC	EC	EC	ECD	ER	ER	EC	PDD
第4のセレクタ	ER	ER	ER	ER	PD	PD	ER	ER

FIG. 5

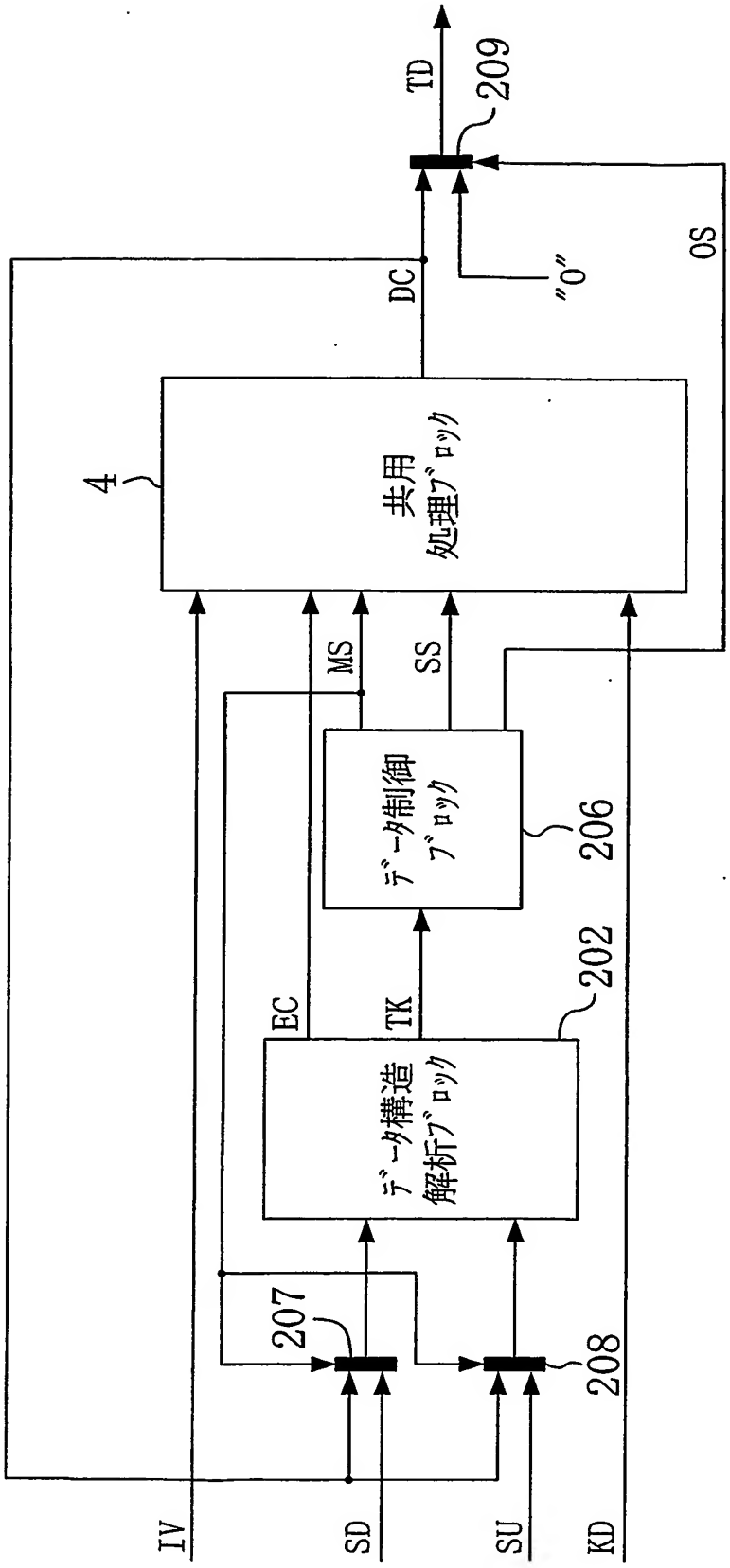
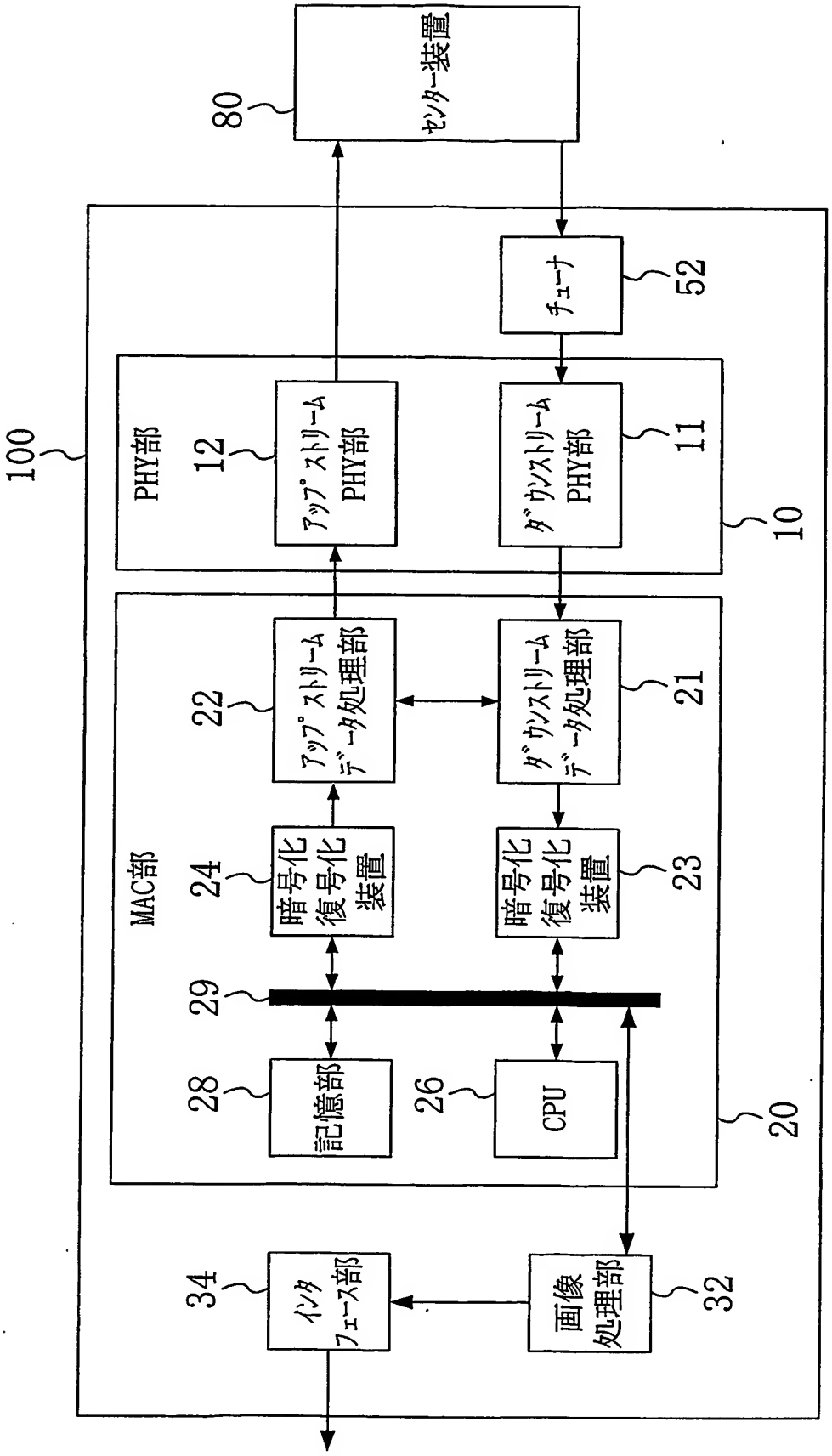

TD
209
DC
"0"
OS
4
共用
処理ブロック
MS
SS
データ制御
ブロック
206
202
EC
TK
データ構造
解析ブロック
207
208
IV
SD
SU
KD

FIG. 6


100
80
センター装置
チューナ
52
PHY部
12
アップストリーム PHY部
ダウンストリーム PHY部
11
10
MAC部
22
アップストリーム データ処理部
ダウンストリーム データ処理部
21
24
暗号化 復号化 装置
暗号化 復号化 装置
23
29
28
記憶部
26
CPU
20
34
インタフェース部
画像処理部
32

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/10186

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/06, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/06, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2000-75785 A (Fujitsu Ltd.), 14 March, 2000 (14.03.00), Full text (Family: none)	1,13,15, 17-20 2,3 4-12,14,16
X Y A	JP 7-261662 A (Fujitsu Ltd.), 13 October, 1995 (13.10.95), Full text (Family: none)	1,13,15, 17-20 2,3 4-12,14,16
Y	JP 2001-177518 A (NEC Corp.), 29 June, 2001 (29.06.01), Full text (Family: none)	2,3

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 October, 2003 (28.10.03)	11 November, 2003 (11.11.03)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/10186

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-215244 A (Sony Corp.), 11 August, 1998 (11.08.98), Full text (Family: none)	2
P,X	JP 2002-297030 A (Toshiba Corp.), 09 October, 2002 (09.10.02), Full text (Family: none)	1,13,15, 17-20

国際調[redacted]告　　国際出願番号[redacted]CT／ＪＰ０３／１０１８６

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ　９／０６，Ｇ０９Ｃ　１／００

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ　９／０６，Ｇ０９Ｃ　１／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００３年
日本国登録実用新案公報	１９９４－２００３年
日本国実用新案登録公報	１９９６－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	ＪＰ　２０００－７５７８５　Ａ（富士通株式会社） ２０００．０３．１４，全文（ファミリーなし）	1, 13, 15, 17-20
Y		2, 3
A		4-12, 14, 16
X	ＪＰ　７－２６１６６２　Ａ（富士通株式会社） １９９５．１０．１３，全文（ファミリーなし）	1, 13, 15, 17-20
Y		2, 3
A		4-12, 14, 16

☒ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 ２８．１０．０３	国際調査報告の発送日 [redacted]
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 石田　信行　[redacted]　5M　9469 電話番号　０３－３５８１－１１０１　内線　３５９８

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ ２００１－１７７５１８ Ａ（日本電気株式会社） ２００１．０６．２９，全文（ファミリーなし）	２，３
Ｙ	ＪＰ １０－２１５２４４ Ａ（ソニー株式会社） １９９８．０８．１１，全文（ファミリーなし）	２
ＰＸ	ＪＰ ２００２－２９７０３０ Ａ（株式会社東芝） ２００２．１０．０９，全文（ファミリーなし）	1, 13, 15, 17-20